On Cyber-Peace

Towards an International Strategy of Cyber-Security

Stefan Schumacher

Magdeburger Institut für Sicherheitsforschung

DeepSec In Depth Security Conference

Über Mich

- NetBSD-Developer, Hacker for almost 20 years
- consultant for IT-Security with focus on Social Engineering, Security Awareness and Counter Intelligence (`www.Kaishakunin.com`)
- Co-Founder and Managing Director of Magdeburger Institut für Sicherheitsforschung `www.sicherheitsforschung-magdeburg.de`
- Co-Editor of Magdeburger Journal zur Sicherheitsforschung
- studied educational science and psychology

Danger

I am not going to present a plan or algorithm to make »the internet« secure, but just some thoughts on IT security from a more global point of view.

strategic level, according to Carl von Clausewitz

On Cyber War

- DeepSec 2010: Cyberwar on the Horizon? Cybercrime/-war
- hype in the media on cyber (in-)security and cyber war
- good: awareness on security is on a high level (at least for some)
- bad: not anyone involved in the discussion knows what he's talking about
- ugly: some journalists, politicians, lobbyist groups (DRM etc.)

Current Development in IT-Security

- IT is emerging to many new fields
- IT security is also emerging to new fields
  but many are not aware of IT security problems
- Electrical and Mechanical Engineers have a complete different concept of security
  static rules published by the organization for standardization (DIN)

Current Development in IT-Security

- IT is emerging to many new fields
- IT security is also emerging to new fields
  but many are not aware of IT security problems
- Electrical and Mechanical Engineers have a complete different concept of security
  static rules published by the organization for standardization (DIN)

the pestilence of modern days ...

- Networking/Internet is emerging to new fields
- IPv6 enables each coffee maker and fridge to be online
- smart living roles out more and more IT
- use your smart phone to control your heating at home and instruct your fridge to order more beer online ...
- once again: it security is expensive and not that sexy, so it is (mostly) ignored
- Cassandra is calling ...

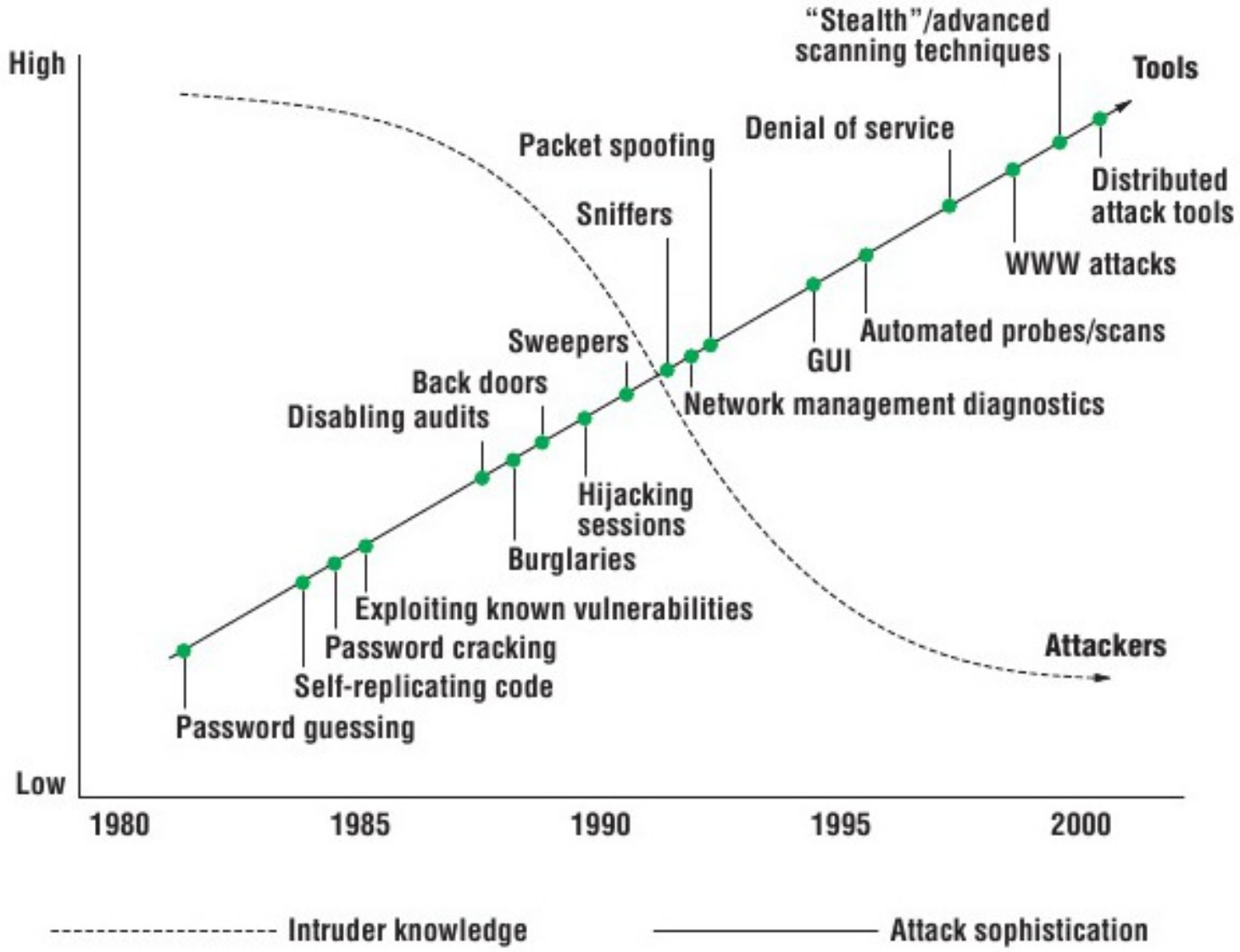
the pestilence of modern days ...

- Networking/Internet is emerging to new fields
- IPv6 enables each coffee maker and fridge to be online
- smart living roles out more and more IT
- use your smart phone to control your heating at home and instruct your fridge to order more beer online ...
- once again: it security is expensive and not that sexy, so it is (mostly) ignored
- Cassandra is calling ...

Stuxnet

- attacked Programmable Logic Controllers (PLC) on Industrial Control Systems
- included the first (created | known) PLC rootkit
- Industrial Control Systems are mainly developed/operated by Electrical Engineers $\rightsquigarrow$ different concept of »security«
- further malicious software might attack other PLCs/ICSs
- a car has been hacked by a manipulated MP3 CD

Attacks - the complete picture



Zombies, Botnets and dDoS

- botnets containing of thousands or even millions of zombies
- used by eg. cyber crime groups to extort companies like banks
- botnets are usually created by automated scanning of large nets and automated exploiting of detected vulnerabilities
- most exploits are already known and patches are available - but not installed
- many average users are still not aware of it security
- if they are aware, they are lacking skills to secure/harden their systems
- according to Microsoft, ca. 40% of exploits use vulnerabilities, where security patches have been available for more than 12 month

Zombies, Botnets and dDoS

- botnets containing of thousands or even millions of zombies
- used by eg. cyber crime groups to extort companies like banks
- botnets are usually created by automated scanning of large nets and automated exploiting of detected vulnerabilities
- most exploits are already known and patches are available - but not installed
- many average users are still not aware of it security
- if they are aware, they are lacking skills to secure/harden their systems
- according to Microsoft, ca. 40% of exploits use vulnerabilities, where security patches have been available for more than 12 month

The Future of Social Engineering

- a technique to circumvent security mechanisms by misusing human behavior
- »Hacking People«
- misuse of fundamental human psychology
- Why should I crack `/etc/master.passwd`, if I can talk a user into revealing his password?

The Future of Social Engineering

- a technique to circumvent security mechanisms by misusing human behavior
- »Hacking People«
- misuse of fundamental human psychology
- Why should I crack `/etc/master.passwd`, if I can talk a user into revealing his password?
- automatic social engineering enhanced spear phishing to collect passwords or install malware (trojans etc.)

The Future of Social Engineering

- a technique to circumvent security mechanisms by misusing human behavior
- »Hacking People«
- misuse of fundamental human psychology
- Why should I crack `/etc/master.passwd`, if I can talk a user into revealing his password?
- automatic social engineering enhanced spear phishing to collect passwords or install malware (trojans etc.)

IT security is multi factorial

- IT security is not just a technological problem
- technological dimension – psychological dimension – social dimension – political dimension – legal dimension
- IT security has to extend its limitations to technology
- cooperation with psychology, social science, educational science, didactics, adult education, law, politics

the human factors ...

- human factors research - a branch of (industrial/engineering) psychology
- man machine interaction, cognitive load of cockpits, electronic assistants in cars
- security awareness and capacity building
- How do I motivate people to get interested in IT security? (huge problem)
- How do I train and educate people in IT security matters? (install patches etc.)
- Want to prevent Social Engineering? $\rightsquigarrow$ social problem $\rightsquigarrow$ social solution $\rightsquigarrow$ psychology
- So there is a lot to do, let's get it on :-)

the human factors ...

- human factors research - a branch of (industrial/engineering) psychology
- man machine interaction, cognitive load of cockpits, electronic assistants in cars
- security awareness and capacity building
- How do I motivate people to get interested in IT security? (huge problem)
- How do I train and educate people in IT security matters? (install patches etc.)
- Want to prevent Social Engineering? $\rightsquigarrow$ social problem $\rightsquigarrow$ social solution $\rightsquigarrow$ psychology
- So there is a lot to do, let's get it on :-)

Manufacturers of Software

- have to deal with security problems
- develop and roll out patches etc.
- get in contact with security researchers, (white hat) hackers
- be aware of security matters

Politics and Law

limited to Germany

- product liability by the manufacturer
- user liability by the user
- users in Germany are normally not responsible/liable for the technical security of their Computers
- but they are responsible/liable for the security of eg. their car
- this should be changed
- the manufacturer of software should also be responsible and liable for their products

Politics

- security policy is an essence of every government (police, firefighters, hospitals, armed forces ...)
- the internet is being discussed by politicians (mostly in a very strange way)
- talk to them, educate them, don't vote for them, found a political party ;-)
- if the manufacturers of software don't care about security, the government could force them ...

nations unite ...

- governments and countries should cooperate in fighting cyber crime
- get aware of cyber crime
- exchange knowledge and technology
- shut down cyber crime gangs

solving solvable problems

some ideas

- according to Microsoft, ca. 40% of exploits use vulnerabilities, where security patches have been available for more than 12 month
- Microsoft evolved and implemented a cyber security strategy (good)
- the users did not evolve (bad)
- Psychology: Awareness, Training, Education
- Politics: make users liable for security problems
- Media: Awarenes, cover the topic (in a serious way!)
- Social Science: Knowledge Management in Organizations

solving solvable problems

some ideas

- according to Microsoft, ca. 40% of exploits use vulnerabilities, where security patches have been available for more than 12 month
- Microsoft evolved and implemented a cyber security strategy (good)
- the users did not evolve (bad)
- Psychology: Awareness, Training, Education
- Politics: make users liable for security problems
- Media: Awarenes, cover the topic (in a serious way!)
- Social Science: Knowledge Management in Organizations

Sum it up

- IT security has many dimensions
- IT security professionals/researchers have to connect to that dimension
- problems can often only be solved in some or all of these dimensions
- IT security is not static!
- Security Exports of the World: Unite!

Sum it up

- IT security has many dimensions
- IT security professionals/researchers have to connect to that dimension
- problems can often only be solved in some or all of these dimensions
- IT security is not static!
- Security Exports of the World: Unite!

Questions?

stefan.schumacher@
sicherheitsforschung-magdeburg.de

9475 1687 4218 026F 6ACF 89EE 8B63 6058 D015 B8EF